

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,

Petitioner,

v.

UMBRA TECHNOLOGIES LTD.

Patent Owner.

Case No. IPR2024-00498

U.S. Patent No. 10,574,482

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I. INTRODUCTION	1
II. ARGUMENT	3
A. Shieh’s Security Processing Modules Are Not <i>Access Point Servers</i> as Alleged in the Petition	3
B. Shieh’s Service Processing Modules Do Not Form Multiple Perimeters as Alleged in the Petition	10
C. Shieh Also Fails to Disclose Multiple Firewall Perimeters Associated with Respective Access Point Servers	15
III. CONCLUSION	16

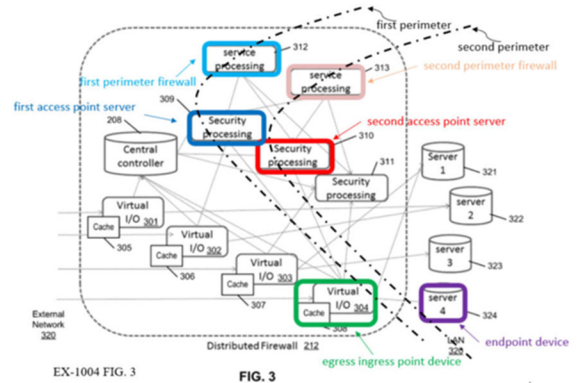
TABLE OF EXHIBITS

- Ex. 2001 RESERVED.
- Ex. 2002 Cisco Business Solutions (2024). Access Point Retrieved on May 13, 2024 from: <https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-access-point.html>.
- Ex. 2003 Microsoft Press (2002). Access Point. In *Microsoft Computer Dictionary Fifth Edition*. Retrieved on May 13, 2024 from: https://burmatarrecords.wordpress.com/wp-content/uploads/2009/12/microsoft_computer_dictionary_fifth_edition1.pdf.
- Ex. 2004 Cisco Internetwork Performance Monitor Glossary (2024). Server. Retrieved on May 13, 2024 from: https://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_internetwork_performance_monitor/2.3/user/guide/glossary.html.
- Ex. 2005 Microsoft Press (2002). Server. In *Microsoft Computer Dictionary Fifth Edition*. Retrieved on May 13, 2024 from: https://burmatarrecords.wordpress.com/wp-content/uploads/2009/12/microsoft_computer_dictionary_fifth_edition1.pdf.

Patent Owner UMBRA Technologies Ltd. respectfully submits this preliminary response to Cisco System, Inc.’s petition seeking *inter partes* review (“Petition”) of U.S. Patent No. 10,574,482 (the “’482 patent”). For the following reasons, the Board should decline to institute *inter partes* review.

I. INTRODUCTION

The centerpiece of the Petition is a heavily annotated version of Shieh’s Figure 3 that adds a “first perimeter” and “second perimeter,” which were both inserted by annotation but are nevertheless shown in black. The “perimeters” are a contrivance of the petitioner and are not described in Shieh. The Petition asserts that the security processing modules (red) are *access point servers* and the highlighted modules (red and blue) collectively create the functional *multi-perimeter firewall* shown by the dashed lines (shown in black, added by annotation).



However, Shieh’s security processing modules are neither *access points* nor *servers*; rather, they are exactly what their name implies. They perform security functions at the behest of other modules. They do not provide access to a network, i.e., they are not access points. Nor do they respond to requests from network clients, i.e., they are not servers.

Secondly, Shieh is clear that a given session's packets are diverted only once to a single security processing module. Shieh *nowhere mentions firewall boundaries or perimeters*, and that makes sense because in Shieh each packet of a given session is diverted to a *single* security processing module. That *single* security processing module can offload tasks to other security modules or service modules, but it provides only a *single* boundary or perimeter because each packet flow communicates directly with only a *single* security processing module. Quite commonsensically, this creates a *single* perimeter, which does not disclose the *multiple* perimeters recited in the challenged claims.

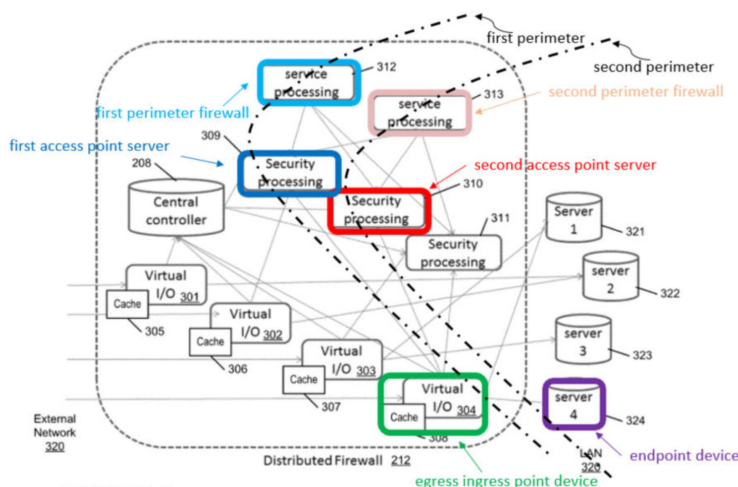
Thirdly, the only modules in Shieh that could possibly provide access point server functionality, (I/O modules), are only deployed singly for any given packet flow. But the patent claims recite (paraphrasing), that a first firewall function is performed proximate one access point server, and then traffic that passes that first firewall is transmitted to the second access point server, where a different firewall function is performed. Given that Shieh never deploys two access point servers in series, the Petition understandably fails to adequately address the use of two access point servers to separate two firewall functions.

Because the Petition fails to address these express claim requirements, it is rife with apparent and conspicuous deficiencies, and the Board should deny institution.

II. ARGUMENT

A. Shieh's Security Processing Modules Are Not *Access Point Servers* as Alleged in the Petition

The Petition alleges that Shieh's security processing module 309 "can be" the recited "first access point server in communication with the egress ingress point device." Petition at 33-34. However, the Petition does not specifically explain how the security processing module 309 qualifies as an *access point server*. Rather, the Petition identifies the security related-functions performed by Shieh's security processing module 309 and notes that, in the preferred embodiment of the '482 patent, an access point server may also "perform firewall services as well":



EX-1004 FIG. 3

FIG. 3

For example, with respect to Annotated FIG. 3, security processing module 309 (blue) can be the *first access point server* in communication with virtual I/O 304 (*egress ingress point device* (green)).³ EX-1004 FIG. 6, 9:9-12 ("In one embodiment, firewall modules 300A-300B could be distributed in different networks, even on different locations,

as long as the modules can reach the module that is next in terms of processing and the central controller.”) Shieh describes that the security processing module 309 may perform firewall services. *EX-1004* 7:53-67. Shieh describes that one of the advantages is that the distributed firewall can employ a significantly large amount of CPU and memory resources for service processing and protect the networks at multiple geometric locations. The central controller decides which security processing module is capable of processing particular connection. *EX-1004* 9:19-26. Shieh discloses that the security processing modules can perform VPN processing which a POSITA understood to be an endpoint of a secure connection or tunnel of a virtual network (*access point servers*). *EX-1003* ¶ 99, *EX-1004* 7:53-55; 7:64-67; 4:14-19. Shieh’s disclosure is consistent with the disclosure of the ’482 Patent which describes that the access point servers are endpoints of a virtual tunnel and may perform firewall services as well. *EX-1001* 2:46-48; 4:43-45; 5:9-13.

Petition at 33-34 (emphases in original).

The Petition next alleges that the security processing module 310 “can be” the recited “a second access point server in communication with the first access point sever.” Petition at 35. Here again, the Petition does not clearly explain how the security processing module 310 qualifies as an *access point server*. Rather, the Petition simply notes that Shieh’s security processing module 310 can send packets to another security processing module.

For example, the *second access point* can be security processing module 310 (red). *EX-1003* ¶ 102. Although not shown in Annotated Figure 3, Shieh discloses that the security processing modules can send packets to another security processing module: “A security processing module receives packets and runs the packets through one or more various security functions in the modules for security processing. There could be several security modules and each handles the same or different security functions. If the packets need to go through another security or service processing, the module sends the packets to the other modules. *EX-1004* 7:53-63.

Petition at 35 (emphasis in original).

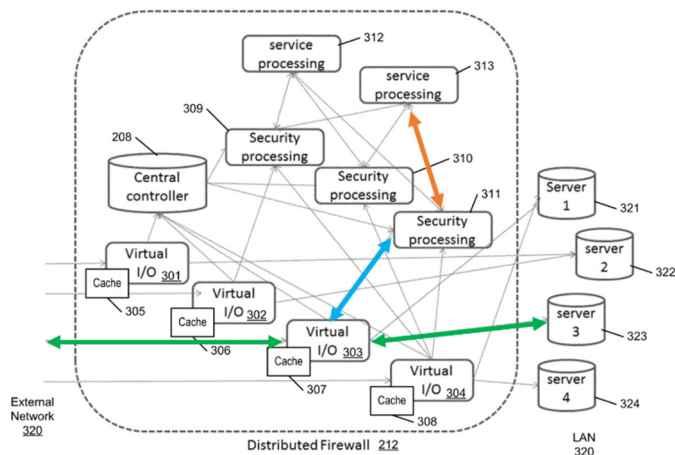
The term *access point server* was well understood at the time of filing and is not given a special meaning or definition in the '482 patent. According to its plain meaning, skilled artisans understand that an *access point server* is a device that responds to other devices and provides services, including an entry point to a network, to the other devices.

An *access point* is, as the name implies, a device that *gives another device an entry point to a network*. According to Cisco, in the context of a wireless network, an *access point* is “a networking device that allows wireless-capable devices to connect to a wired network.” Ex. 2002. The Microsoft Computer Dictionary defines access point similarly, also in the context of a wireless network: “In a wireless LAN (local area network), a transceiver that connects the LAN to a wired network.” Ex.

2003. Both definitions are consistent with the usage of the term access point server in the '482 patent. Ex. 1001 at 12:1-10, 14:13-16 (wherein the access point servers are described as providing access to the network to end point devices).

A *server* is a device that responds to and provides services to another device on the network, usually called a client device. According to a Cisco definition, a *server* is “a node or software program that provides services to clients.” Ex. 2004. The Microsoft Computer Dictionary defines a *server* as follows: “On the Internet or other network, a computer or program that responds to commands from a client.” Ex. 2005. Both definitions are consistent with the usage of the term access point server in the '482 patent. Ex. 1001 at 5:7-15, 8:61-65, 11:62-12:10 (wherein the access point servers are described as responding to requests from end point client devices to provide access to a network).

The Shieh security processing modules 309/310 identified in the Petition as the claimed “access point server[s]” are not devices that respond to other devices and provide services to them, including an entry point to a network. Rather, in Shieh, any such functionality is provided to external devices by the virtual I/O modules 301-304. Referring to the annotated version of Shieh’s Fig. 3 to the



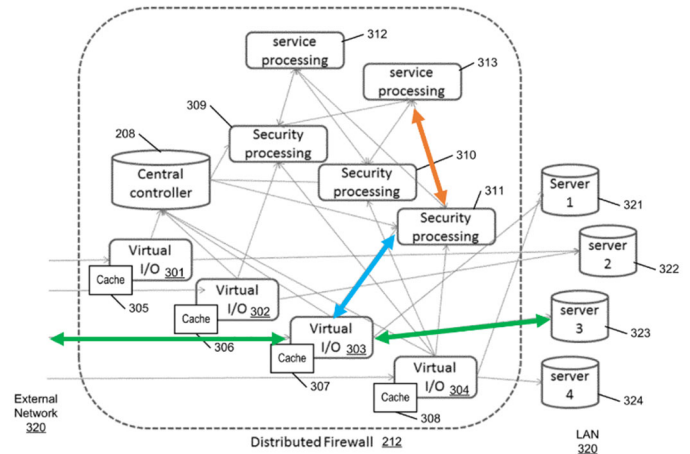
right, Shieh explains that packets are transmitted to and from the external network 320 [sic, 315¹] to the LAN 320 **along the path shown in green**. Ex. 1004 at 7:32-35 (“Each of virtual I/O modules 301-304 receives packets from any of servers 321-324 of LAN 320 and sends packets to external network 315 outside of the firewall.”) The I/O module then performs a table look-up and **sends the packet to the specified security processing module**. *Id.* at 7:42-45 (“Upon receiving a packet, an I/O module performs a packet classification to find out the associated connection and forwards the packet to the corresponding security processing module identified by the forwarding table.”) The security processing unit 311 sends the packet back to the I/O module 303 or, alternatively, it can send the packet directly to the destination (server 323 in the illustrated example) if it is configured to do so. *Id.* at 7:64-67 (“If a [security processing] module is the last processing module in the chain to process the packets, it can forward the packets back to the virtual I/O module to send out, or send the packet out directly to its destination if it’s configured to do so.”)

Shieh explains that if the security processing module 311 cannot perform a required function (e.g., due to resource limitations), it can **“outsource” the function to an optional service processing module 313**, which sends the packets back to security processing module 311 when the service is complete. *Id.* at 8:4-13

¹ Shieh’s specification identifies the external network as external network 315. Ex. 1004 at 7:34.

(“However, [the *service* processing module] is different from the *security* processing module in that it only receives and sends packets to the same security processing module. If the tasks cannot be done in a security processing module, for example, due to a resource limitation, system load, or the requirement of a different operation system, the packets can be forwarded to one or more of service processing modules 312-313 for further processing. The packets then are sent back to the same security processing module for the next security function processing.”) (emphasis added). The service processing modules are optional components and are not part of the typical or core communication path. *Id.* at 8:39-42 (“Note that a *service processing module is optional in the architecture*, as it is only required when there are needs to use additional resources to handle the security functions.”) (emphasis added). Because Shieh’s security processing modules 310/311 do not respond to and provide services to other devices, including an entry point to a network (rather they process security functions *within* a network), they cannot be the recited *access point servers*.

Further, the security processing modules 309/310/311 are not *servers* to devices not already in a network and thus cannot qualify as the recited access point servers for this additional reason. The Shieh security processing modules are part of distributed firewall system 212 which connects an end point in an external network 315 to one of the servers 321-324 (i.e., “Server 1,” “Server 2,” “Server 3,” “Server 4”). The servers are labelled as such. As noted above, the security processing modules can optionally forward packets to one of the servers 321-324 on behalf of a paired virtual I/O module 301-304 if configured to do so, but that does not make them servers. For example, the security processing modules can forward received packets to a given destination if so instructed by a controller but neither “respond to” nor “provide[] services to” such destination as set forth in the foregoing definitions of server. *See* Ex. 2005, Ex. 2006. Shieh’s security processing modules thus are not *servers*.



Given that the Petition fails to explain how Shieh’s security processing modules are either *access points* or *servers*, much less the claimed “access point server[s],” they cannot meet the access point server limitation. The petition should be denied for this reason.

B. Shieh’s Service Processing Modules Do Not Form Multiple Perimeters as Alleged in the Petition

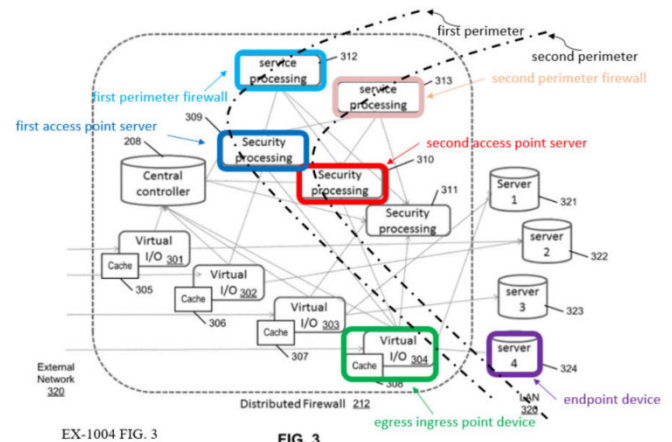
The Petition alleges that Shieh’s *service* processing modules 312/313 (not to be confused with the *security* processing modules 309-311) are the recited “first perimeter firewall in communication with the first access point server” and “second perimeter firewall in communication with the second access point server.” Petition at 36, 39-40. The Petition argues that the service processing modules 312/313 meet the claims because they are “located functionally” at different places between the internal network 320 and external network 315 (misabeled 320 by Shieh in the figure):

Shieh discloses that service processing module 312 (light blue) (*first perimeter firewall*) performs one or more of the security functions for the security processing module 310

(red) (*first access point server*). EX-1004 8:1-13. As shown in

Annotated FIG. 3 [provided on the right by Patent Owner], service processing module 312 is located functionally at a perimeter between an internal network 320 and an

external network 315. *EX-1004* 7:31-52. Shieh discloses that that the distributed firewalls can be located at multiple boundaries in the cloud between a client location and their link to the internet. With reference to Annotated FIG. 3, a first perimeter (dashed black line) can be



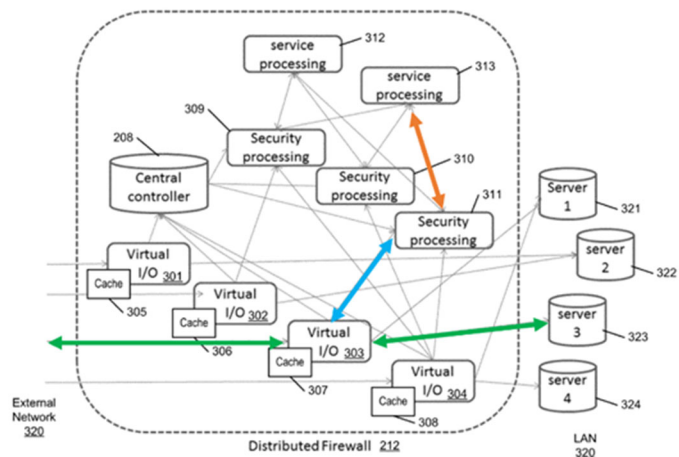
located in a cloud where the security processing module 309 and the service processing module 312 are located in the same location, and a second perimeter (dashed black line) can be located in a cloud where the security processing module 310 and the service processing module 313 are located in a different location so long as the two security processing modules are in communication with each other. *EX-1004* 9:9-11. This is consistent with the '482 Patent's disclosure that the firewalls are virtualized in the cloud and the perimeters are located between the client and the internet at each firewall. *EX- 1001* 11:17-25; 13:64-14:4

...

As discussed above with respect to limitation [1.5], and as shown in Annotated FIG. 3, service processing module 313 is located functionally at a second perimeter (dashed black line) between an internal network 320 an external network 315. *EX-1004* 7:31-52.

Petition at 36-37; 40 (emphasis in original).

As explained in the preceding section, the *service* processing modules are optional modules that can perform a given function for a *security* processing module if that *security* processing module, for instance, is resource constrained. *Ex. 1004* at 8:4-13, 39-42. (“However, [the

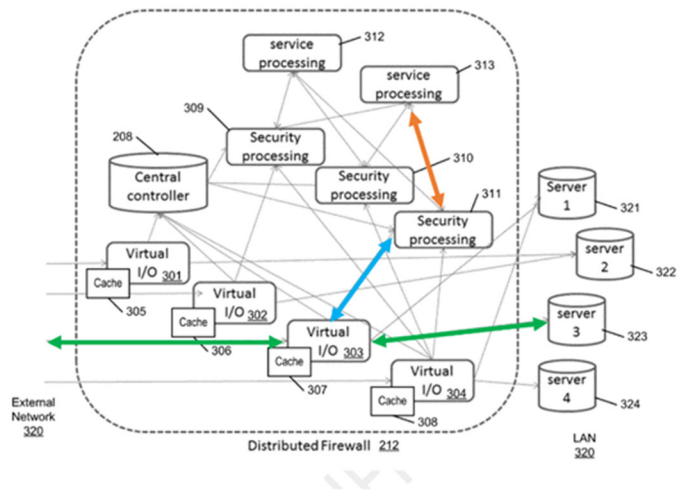


service processing module] is different from the *security* processing module in that it only receives and sends packets to the same security processing module. If the tasks cannot be done in a security processing module, for example, due to a resource limitation, system load, or the requirement of a different operation system, the packets can be forwarded to one or more of service processing modules 312-313 for further processing. The packets then are sent back to the same security processing module for the next security function processing. . . . Note that a service processing module is optional in the architecture, as it is only required when there are needs to use additional resources to handle the security functions.”) (emphasis added).

Thus, Shieh’s service processing modules do not and cannot define any functional perimeter or border. A service processing module is “visible” only to the central controller 208 and the particular *security* processing module that is offloading a task to that particular *service* processing module. The service processing module is optional and is invisible to the remainder of the network. It therefore cannot create any functional perimeter.

Further, the distributed firewall 212 of Shieh only creates a single perimeter or boundary to protect the network entrance. Shieh’s only teaching on the issue is “[b]y dividing a firewall into different modules, it allows putting virtual I/O and security processing functions at the best locations to protect the network entrance, while keeping the central control and monitoring functionality at the central

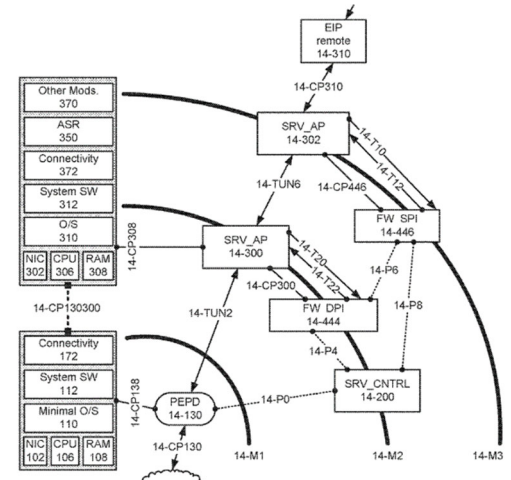
controller.” *Id.* at 8:33-37. **Shieh** nowhere uses the terms *boundary* or *perimeter* or otherwise addresses firewall boundaries or perimeters. Shieh explains that a packet is received by an I/O module and is forwarded (under the direction of the controller 208)



to a *single security processing module*. That security processing module optionally offloads a security task to a *service* processing module or other security processing modules, but the other “helper” module(s) are chained together so as to send the packet back to the original requesting virtual I/O module (unless, and optionally, the packet is leaving the network). *Id.* at 7:60-62, 64-67.

Accordingly, for a given session, there is only a single security processing module (module 311 in the example illustrated above right) that communicates directly with the access point server (the I/O module 303 in this example) to initiate a single security processing. Depending on load and capabilities, security processing module 311 may offload certain tasks to other modules, but the results are sent back to I/O module 303 for the illustrated session. *Id.* The Shieh system does not and cannot form multiple functional perimeters. Consistent with this, Shieh nowhere discusses the concept of providing multiple security *perimeters* or *boundaries*.

In contrast, the claims of the '482 patent recite that the firewalls establish two distinct perimeters. The preamble of each independent claims recites “[a] multi-perimeter firewall system.” Ex. 1001 at 25:3, 27:1. The body of each independent claim recites a “first perimeter firewall” in communication with a first access point device, a “second perimeter firewall” in communication with the second access point device, and that the two access point devices are in communication with one another. *Id.* at 26:5-6, 10-11; 27:10-11, 16-17. It should be noted in this connection that, according to the '482 specification, the first perimeter firewall 14-446 can be deployed within the first access point server 14-302 and the second perimeter firewall 14-444 can be deployed within the second access point server 14-300. *See id.*, FIG. 14 (a portion of which is shown above right).



Consistent with the foregoing, the title of the patent is “Multi-perimeter Firewall in the Cloud” and the Field of the Disclosure and Summary of the Disclosure each state that the disclosure is directed to multi-perimeter firewalls. Ex. 1001 at 1:15-19; 2-36-37 (Field of the Disclosure: “The present disclosure relates generally to networks, and more particularly, network security which protects the flow of traffic through a global virtual network or similar network by the strategic

positioning of distributed firewall (FW) devices placed at multiple perimeters in the cloud.” Summary of the Disclosure, first sentence: “Systems and methods for providing multi-perimeter firewalls via a virtual global network are disclosed.”) All embodiments described in the detailed description of the ’482 patent specification include firewalls forming multiple discrete perimeters.

For these reasons, the claims as properly construed according to their ordinary meaning require at least two firewalls that create distinct perimeters.

Shieh’s specification is clear in this regard – it does not disclose a system having two firewalls that create distinct perimeters. Patent Owner submits that this is another example of the Petition failing to address an apparent discrepancy between its argument and the clear teachings of the primary reference. The petition should be denied for this additional reason.

C. Shieh Also Fails to Disclose Multiple Firewall Perimeters Associated with Respective Access Point Servers

In the preceding sections, Patent Owner explained how Shieh’s security processing modules are not *access point servers* and that the only components of Shieh that could perform firewall functions are never connected to multiple perimeters.

Relatedly, the independent claims recite that the first firewall “prevent[s] at least some traffic from passing from the first access point server to the second access point server” and that the second firewall “prevent[s] at least some traffic from

passing from the second access point server to the end point device.” Ex. 1001 (claim limitations 1.5-1.6 and 13.5-13.6). The plain meaning here is that a first firewall function is performed proximate one access point server, and then traffic that passes that first firewall is transmitted to the second access point server, where a different firewall function is performed.

Shieh’s I/O modules (*i.e.*, the components that could qualify as access point servers) do not communicate with one another, but independently bridge between networks 315 and 320. Ex. 1004 at 32-35. Thus, as explained above, in Shieh a given packet stream travels through only a single I/O module. Knowing that Shieh never forms the configuration of the claims, Petitioner attempted to avoid equating the I/O modules to access point servers. But there are no other modules in Shieh that provide an entry point to the network for other devices, thus the Petition cannot be correct.

Shieh’s I/O modules thus cannot meet recitations that require packet flow between two access point servers, between the two distinct firewall functions. For this further reason, the Petition should be denied.

III. CONCLUSION

For the foregoing reasons, Patent Owner UMBRA Technologies Ltd. respectfully submits that the Board should decline to institute *inter partes* review in this proceeding.

Dated: May 13, 2024

Respectfully submitted,

By: /James E. Harris/

James E. Harris
Reg. No. 40,013
GARDELLA GRACE P.A.
2502 North Clark Street, Suite 222
Chicago, IL 60614
Phone: 703-773-4933
Fax: 703-740-4541
jharris@gardellagrace.com

Greg H. Gardella
Reg. No. 46,045
GARDELLA GRACE P.A.
80 M Street SE, 1st Floor
Washington, D.C. 20003
Phone: 703-721-8379
Fax: 703-740-4541
ggardella@gardellagrace.com

*Attorneys for Patent Owner
UMBRA Technologies Ltd.*

WORD COUNT CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(d), I hereby certify that the foregoing
PATENT OWNER'S PRELIMINARY RESPONSE contains 3,399 words as
measured by the word processing software used to prepare the document. This
total does not include the table of contents, the caption page, the table of exhibits,
any signature blocks, the certificate of service, or this certificate of word count.

Respectfully submitted,

Dated: May 13, 2024

By: /James E. Harris/

James E. Harris
GARDELLA GRACE P.A.

CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing PATENT OWNER'S PRELIMINARY RESPONSE along with EXHIBITS 2002-2005 were served in their entirety by filing the documents through the Patent Trial and Appeal Case Tracking System (P-TACTS) as well as providing courtesy copies via e-mail to the following attorneys of record for the Petitioner listed below:

Patrick D. McPherson
Patrick Muldoon
Joseph Powers
DUANE MORRIS LLP
901 New York Avenue N.W., Suite 700 East
Washington, DC 20001
Telephone: 202-776-5214
Email: PDMcPherson@duanemorris.com
Email: PCMuldoon@duanemorris.com
Email: JAPowers@duanemorris.com

Dated: May 13, 2024

By: /James E. Harris/

James E. Harris
GARDELLA GRACE P.A.